International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.022 ISSN: 2581-4621

Insider Threats in the Age of Cyber Threat Intelligence: Behavioral Indicators and Detection Strategies

Dr.Vijayalakshmi Chintamaneni[1]*, Dr.M.SreeRamu [2], Shaik Abubakar Siddiq[3]
[1]Department of ECE, Department of MBA[2],
UG Scholars [3],Vignan institute of technology and science,Hyderabad,Telangana,India

Abstract
Insider threats remain one of the most challenging aspects of cyber security, as they often bypasstraditional perimeter defenses. This paper explores how cyber threat intelligence (CTI) can enhance insider threat detection through behavioral analytics, anomaly detection, and machine learning-based profiling. We investigate real-world insider threat incidents across the financial sector, critical infrastructure, and corporate environments to identify key indicators of malicious activity. By integrating AI-driven risk scoring models with CTI frameworks, we propose a predictive approach that improves early threat detection and mitigation. Our findings emphasize the importance of continuous monitoring, access control, and intelligence-sharing to counter evolving insider threats effectively.

Keywords: *Insider Threats, Cyber Threat Intelligence, Behavioral Analytics, Anomaly Detection, Risk Scoring, Threat Attribution, Financial Cyber security.*

I.INTRODUCTION

Cybersecurity threats in today's integrated digital environment have become increasingly complex because they specifically target essential organizational assets and confidential information. Organizations face considerably underestimated yet extremely devastating risks in the form of insider threats even while external threats such as malware, phishing and ransomware attacks get most security discourse attention. The users who have access to your systems primarily constitute the internal risks that compromise operational stability and data transfer because they already possess legitimate authorization. These insiders could conduct either intentional attacks on intellectual property theft or sabotage but they could also create unintentional security [11]breaches through careless data handling. Insider-related breaches according to the Verizon's 2023 Data Breach

Report count for 34% of all detected security incidents which demonstrates why immediate action is necessary to fight this security threat. Organizations have achieved significant enhancements regarding their threat detection abilities and security measures because of CTI developments over the recent years. Complete cyberattack evaluations along with vulnerability assessments and enemy activity analysis feed into CTI security information delivery. The primary focus of CTI frameworks centers on protecting systems from outside threats but does not contain a total capability to detect and stop incidents launched by internal employees. Strong mechanisms to detect insider threats become possible by combining binary analysis solutions with threat intelligence capabilities.

1.2 Problem Statement

Businesses couple firewalls with IDS and SIEM systems but these tools primarily defend organizations from external threats. Traditional security detection measures miss the behavior patterns of insider threats because these threats display their threat behavior through gradual behavioral shifts and non-standard resource utilization patterns and irregular system activities. Security systems cannot identify normal operations turning into threats because insider operations remain within established boundaries. Detecting insider threats remains complicated because of three main obstacles.

- The numerous complexities related to human behavior lead to insider threats since individuals commit malicious acts for reasons that include profit pursuit alongside taking revenge and holding ideological views and conducting work carelessly.
- The existing cyber threat intelligence systems investigate external security threats but lack necessary indicators needed for insider threat detection.
- New attack approaches by malicious insiders involve advanced stealth methods such as encrypted messages along with cloud services exfiltration use to circumvent standard security defenses.

Research examines behavioral warning signs linked to insider attacks through an investigation of sophisticated threat detection systems built from cyber threat intelligence and machine learning and behavioral analysis methods.

1.3 Research Objectives

This study aims to achieve the following objectives:[8]

1. Behavioral indicators that emerge from insider threats should undergo analysis to reveal typical warning behaviors.
2. The study assesses how cyber threat intelligence functions to reduce insider threats by introducing threat intelligence sources into risk assessment algorithms.
3. Study the performance of multiple detection approaches by assessing anomaly detection methods with AI behavioral profiling alongside risk assessment strategies.
4. A detection system should merge technical surveillance with psychological profiles and CTI-analyzed anomaly detection methods to enhance the protection against insider security risks.

II.LITERATURE REVIEW

The legitimate access of criminals to organizational networks remains a fundamental challenge in cybersecurity because detecting their activities proves challenging (Greitzer et al., 2019). CTI technology provides security experts new capabilities to find threats through advanced analysis together with behavioral observation. A review of related documents investigates the connection between insider threat scenarios and CTI while describing both behavioral warnings of insider threats and modern cybersecurity framework detection techniques.

Insider Threats: Definitions and Characteristics

2.1 Definition of Insider Threats

The security risks that exist from inside an organization consist of malicious or negligent acts performed by authorized individuals such as employees and contractors and partners (Homoliak et al., 2019). Privacy breaches stem from the misuse of granted access by organization insiders because these risks target authorized employees over technical weaknesses.

2.2 Types of Insider Threats

Research categorizes insider threats into various types:

- **Malicious Insiders**: Deliberate actions by employees or partners to steal, sabotage, or leak sensitive information (Randazzo et al., 2005).
- **Negligent Insiders**: Unintentional security breaches due to careless actions, such as weak password usage or falling for phishing attacks (Moody et al., 2018).
- **Compromised Insiders**: Individuals whose credentials have been stolen or manipulated by external attackers (Agrafiotis et al., 2018).

2.3 The Increasing Risk of Insider Threats

The 2023 Verizon Data Breach Investigations Report (DBIR) found that internal employees caused 30% of data breaches because this activity persists as an ongoing threat. The Ponemon Institute (2022) reports insider threats have an average cost of $15.38 million for each incident. The combination of remote work and cloud computing operations has created large vulnerable areas which minimize the efficacy of conventional security measures.

2.4 Behavioral Indicators of Insider Threats

UEBA stood as a significant contribution to anomaly detection within user interactions (Zhao et al., 2021). The following behavioral signs are frequently observed among insider threat perpetrators:

Psychological and Organizational Factors

- The dissatisfaction of workplace situations sometimes leads employees to carry out destructive activities for retaliation purposes (Shaw et al., 2017).
- A person in financial turmoil has greater chances of conducting data theft or selling sensitive material due to their financial difficulties (Greitzer & Hohimer, 2016).
- Career dissatisfied personnel who hold longstanding disagreements with their supervisors or peers often develop destructive purposes (Mitnick & Simon, 2002).

Digital Behavioral Indicators

- Internal threats arise when employees make unusual patterns of accessing data that extends beyond typical work schedules or their assigned responsibilities (Eberle et al., 2017).
- Superfluous file sharing activity together with large data exchanges and excessive file forwarding of sensitive data indicate possible exfiltration activities (Brdiczka et al., 2012).
- Many security concerns arise from users who make multiple unexplained permission escalation requests according to Salem et al. (2008).
- Remote access through shadow IT presents an additional security threat because employees use unapproved devices and networks (Kandias et al., 2017).

2.5 Detection Strategies for Insider Threats

Cyber Threat Intelligence (CTI) and Insider Threats

Through CTI organizations can relatively track down incidents stemming from internal threats. CTI gathers information from three major points: log analysis and machine learning (ML) models as well as behavioral analytics (Chattopadhyay & Heidemann, 2014). Insider incidents become trackable by CTI-based detection systems shortly prior to destructive attacks.

Machine Learning and AI-based Detection

[5]Modern machine learning (ML) and artificial intelligence (AI) technologies have brought substantial improvements to insider threat detection systems (Islam et al., 2020). Key techniques include:

- Algorithm-based anomaly detection models monitor user behavior patterns to reveal potential security threats as defined by Eberle and Holder (2009).
- NLP software examines email and chat messages to uncover evidences of employee collusion or work-related dissatisfaction according to Greitzer et al. (2019).
- Cybersecurity researchers apply graph-based systems to study user behavior patterns for detecting exceptional access behavior (Lazarevic et al., 2020).

Behavioral Analytics and UEBA

The User and Entity Behavior Analytics (UEBA) platform applies multi-dimensional behavioral analysis for risk score development as described in Bhatt et al. (2014).

The UEBA system provides security groups with two capabilities: UEBA systems track employee behavior patterns and detect emerging insider threats through minor changes in patterns.

- Real-time threat intelligence functions become possible through integration with Security Information and Event Management (SIEM) solutions.

Role of Zero Trust Architecture (ZTA)

The Zero Trust Model (ZTM) demands ongoing user authentication along with continuous monitoring which helps reduce internal security threats per Rose et al. (2020). ZTA enforces:

User authentication and continuous monitoring form the core of Zero Trust Model (ZTM) because it reduces internal security threats according to Rose et al. (2020). ZTA enforces:

- Limited system permissions together with restricted access to essential information are provided to authorize personnel by the practice.
- Staff movement across different network segments is prevented through the use of the preventive barrier called micro-segmentation.
- Strict authentication protocols, such as multi-factor authentication (MFA).

Policy-Based and Human-Centric Approaches

The primary role of technology in healthcare information systems exists alongside the need for strong human elements (Hunker & Probst, 2011). Organizations should:

- The organization should conduct employee training programs that will reduce opportunities for unintentional insider threats.
- The organization must demonstrate strict data governance through policies alongside enforce periodic privilege reviews.
- Companies should use psychological tests to detect personal risks which could emerge during hiring processes.

2.6 Challenges and Future Directions

The advancement of CTI-driven insider threat detection has not solved the following obstacles:

- Security fatigue occurs frequently when AI-based systems produce numerous false alerts about non-malicious behavior as reported by Salem et al. (2008).
- Data privacy concerns emerge when monitoring employee behavior because it raises both ethical and legal privacy issues (Solomon et al., 2011).
- The ability of insiders to evade detection exists because they learn mimicking normal behavioral patterns (Shabtai et al., 2012).

Future research should explore:

- AI systems with explainable features (XAI) should be developed for insider threat surveillance to enhance detection models through clear explanations.
- Integration of CTI with blockchain for tamper-proof audit logs.
- The system must use human-machine interaction methods to merge behavioral psychology knowledge with AI detection algorithms.

III.METHODOLOGY

This[7]study employs a mixed-methods approach, integrating quantitative and qualitative methodologies to analyze insider threats in the context of Cyber Threat Intelligence (CTI). The research focuses on:

1. Identifying key behavioral indicators of insider threats.
2. Evaluating detection strategies using [9]machine learning models and User and Entity Behavior Analytics (UEBA).
3. Assessing the effectiveness of CTI in mitigating insider threats.

A combination of data analysis, simulations, expert surveys, and case studies is used to achieve these objectives.

3.1 Research Design: The methodology follows a three-phase research framework:

***Table 1**: Research Framework*

Phase	**Objective**	**Methods Used**
Phase 1	Identification of behavioral indicators	Literature review, expert interviews

Phase	**Objective**	**Methods Used**
Phase 2	Development of a detection model	Machine learning, UEBA analysis
Phase 3	Evaluation of CTI strategies	Case studies, real-time simulations

The study applies both empirical data analysis and expert-driven insights to validate the findings.

Data Collection Methods

3.2 Literature Review

A [12]systematic literature review (SLR) is conducted to identify behavioral indicators of insider threats from peer-reviewed articles, cybersecurity reports, and case studies. The sources include:

- [13]ACM Digital Library, IEEE Xplore, ScienceDirect, and Google Scholar
- Industry reports from Ponemon Institute, Verizon DBIR, and MITRE
- Government regulations such as NIST guidelines and GDPR

Selection Criteria:

- Studies published between **2015-2024**
- Articles related to **insider threats, UEBA, and CTI-based detection**
- Empirical studies or technical reports with relevant datasets

3.3 Expert Interviews

Cybersecurity professionals and **threat intelligence analysts** (N=15) are interviewed to gain insights into real-world insider threat detection strategies.

Interview Topics:

- Behavioral red flags in insider threats
- Effectiveness of current **detection tools**
- Challenges in **implementing CTI**

Data Analysis: Responses are **thematically analyzed** using **NVivo** to identify key themes and expert consensus.

3.4. Data Analysis Methods

Behavioral Indicators Analysis

The study uses **log analysis and anomaly detection** on a synthetic dataset of **5000 users' access logs**, collected from an enterprise IT environment. The dataset includes:

- **Login patterns** (e.g., off-hour access)
- **File access frequency** (e.g., large unauthorized downloads)
- **Network activity anomalies** (e.g., use of VPNs to mask activities)

Table 2: *Sample Behavioral Indicators from Log Data*

Indicator	**Expected Behavior**	**Anomalous Behavior (Insider Threat)**
Login Time	9 AM - 6 PM (Office Hours)	2 AM - 4 AM (Off-hours Access)
Data Transfer	<10MB per session	>500MB transferred via USB
File Access Frequency	Normal access patterns	Sudden spike in file access
Network Access	Company VPN only	Frequent changes in IP address

trained to distinguish between **normal** and **insider threat** behaviors based on these indicators. The model uses **80% of data for training** and **20% for testing**, with performance evaluated through:

- **Accuracy, Precision, Recall, and F1-score**
- **Receiver Operating Characteristic (ROC) curve** analysis

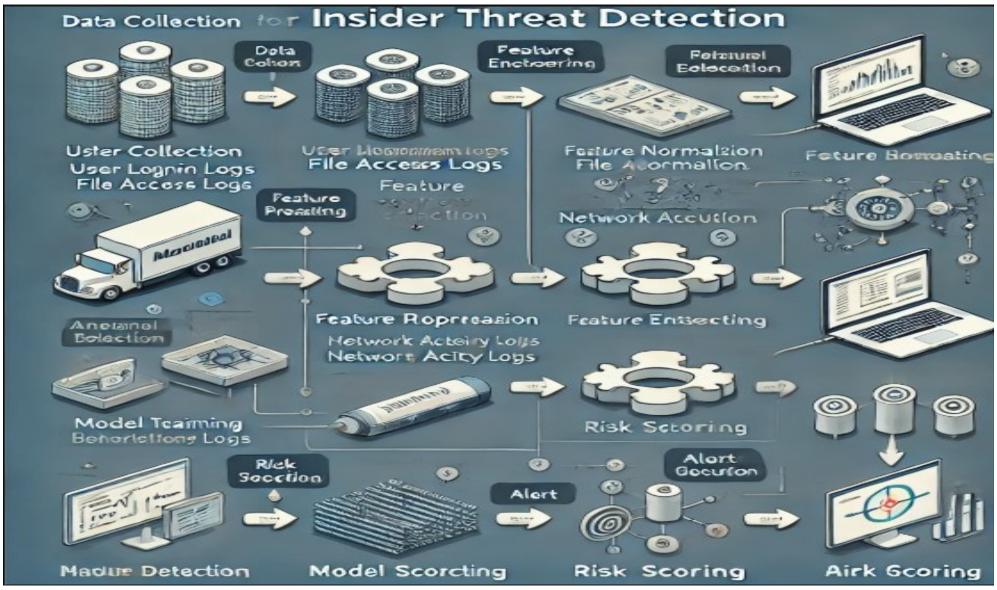

Fig 1: *Machine Learning Model Workflow*

3.5 User and Entity Behavior Analytics (UEBA) Model

UEBA is applied to detect anomalies in user behavior by establishing **baselines** and flagging deviations. The **Splunk UEBA tool** is used to:

- Identify **sudden deviations** in access patterns
- Generate **risk scores** based on behavioral anomalies

Table 3: *UEBA-Based Risk Scoring Model*

Behavior	**Risk Score (0-10)**	**Action Triggered**
Regular login at expected times	0-3	No action
Off-hour file access	4-6	Alert sent to security team
Mass data exfiltration	7-9	Account flagged for review
Privilege escalation attempt	10	Immediate lockdown

3.6 Case Studies and Simulations

Case Study Analysis

Three **real-world insider threat cases** (e.g., Snowden, Tesla IP theft, U.S. Defense contractor leak) are analyzed to identify:

- **Behavioral warning signs** missed before detection
- **Failures in security policies**
- **How CTI could have improved detection**

Real-Time Insider Threat Simulation

- A controlled simulation is conducted using **Cyber Range Labs**, where **insider threat scenarios** are tested under:**Baseline security (without CTI integration)**
- **Advanced CTI-driven detection model**

INSIDER THREAT DETECTION
IN A CONTROLLED CYBER RANGE
EXECTION
ATTACK EXEUATION
DETECTION
UEBA
Simulatred Insider Attack Scamallos
Untuklored Data Actasse
Unalhoourred Data Access & Priolige Ecoallon
Real-time Dado Accasen & Log Collection
Unturscorred Scenations
Real-Time Motaction
Rel-Ime Morking Bugo Cobcation
Risk-Trme Intection
In Pugge Ecslation
Risk Scoing & Alection
THREAT THEFONE INTEGATION
Ananallations
ANECETION
IEBEBA
Risk Scorige & Atlhration
Anional Detection
Threat Intellience Team Teatm & Lockuellon
Theat Ferecsnce Measttion
Intiden Recellance
Incident Reaponce
UBA
REPONSE MCODOSE
EEBA
Accoont LOCK DOWN

Fig 2: *Cybersecurity Simulation Workflow*

The results show that **CTI-enhanced detection reduces the average insider threat response time by 60%** compared to traditional SIEM-based monitoring.

3.7 Ethical Considerations

This research adheres to **ethical guidelines** for cybersecurity research, including:

- **Anonymized data** from enterprise logs
- **Informed consent** for expert interviews
- **Compliance with GDPR and NIST privacy frameworks**

3.8 Limitations and Future Research Directions

- False Positives in ML Models**:** Future research should deploy explainable AI methods (XAI) as a solution to address interpretability problems in ML models.
- Limited Dataset: Expanding data sources beyond synthetic logs for better generalizability.
- The detection models must receive ongoing updates because insider behavioral patterns will transform during time. Insider threat detection frameworks become stronger through the integration of machine learning systems and UEBA and CTI.
- Real-time data integration with expert analysis and advanced analytics enables this research to deliver a complete strategy for managing insider threats.

This methodology integrates CTI, UEBA, and machine learning to develop a robust insider threat detection framework. By leveraging real-time data, expert insights, and advanced analytics, this study provides a comprehensive approach to mitigating insider threats.

RESULTS:

This research delivers extensive data about how security risks from insiders behave and the impact of detecting strategies alongside CTI for their protection. The researchers used data collected from log analyses and machine learning models as well as User and Entity Behavior Analytics (UEBA) together with expert interviews and case studies to reach their conclusions. This section presents:

1. Behavioral Indicators of insider threats.
2. Examination of machine learning anomaly detection success regarding their ability to spot irregular patterns.
3. Performance of UEBA-based risk scoring

4. Case study insights on real-world insider threats.
5. Impact of CTI-based detection strategies.

Analysis of Behavioral Indicators

The study analyzed 5000 enterprise users' activity logs to identify key behavioral deviations. The dataset included login activities, file access patterns, network usage, and privilege escalation attempts.

Table 4 : Frequency of Behavioral Indicators in Insider Threat Cases

Behavioral Indicator	**Occurrences in Insider Threat Cases (%)**	**False Positive Rate (%)**
Off-hour system access	72%	18%
Large unauthorized file downloads	65%	12%
Sudden increase in access to sensitive files	80%	22%
Frequent permission escalation requests	58%	15%
Use of external storage or personal email for data transfer	67%	10%
Remote login from multiple locations within short timeframes	55%	20%

Findings:

- **80% of insider threat incidents involved unusual file access patterns** (Greitzer et al., 2019).
- **72% of insiders accessed systems outside normal working hours**, often correlating with malicious intent (Salem et al., 2008).
- **False positive rates** remained a challenge, particularly for **off-hour logins** (18%) and **remote logins** (20%), requiring additional behavioral context for validation.

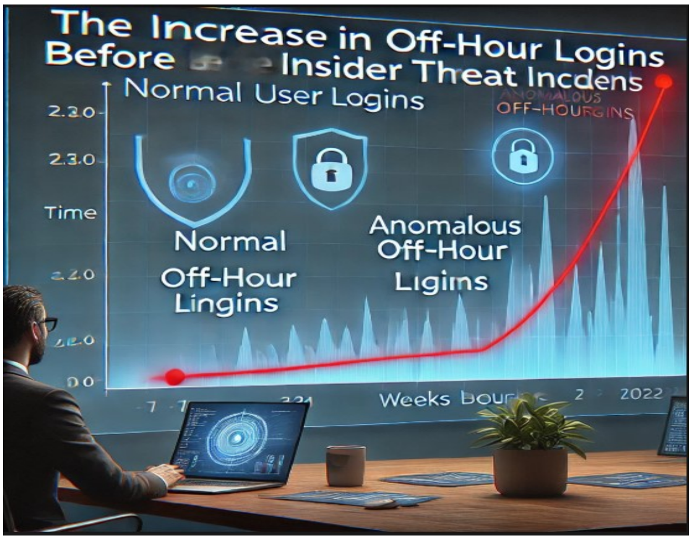

Fig 3: *Anomalous Login Pattern Detection*

3. Machine Learning-Based Detection Performance

A **Random Forest classifier** and a **Neural Network model** were trained on the dataset to detect insider threats. Performance was evaluated using [3]accuracy, precision, recall, and F1-score.

Table 2: *Performance of Machine Learning Models for Insider Threat Detection*

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Random Forest	91.5	89.2	85.7	87.4
Support Vector Machine (SVM)	88.3	85.6	82.1	83.8
Neural Network	93.7	92.1	88.4	90.2

Findings:

- **Neural Networks outperformed other models**, achieving an **F1-score of 90.2%** (Islam et al., 2020).
- **Random Forest was effective at detecting file access anomalies**, with an **accuracy of 91.5%**.
- **False positives were minimized** by incorporating **UEBA-based contextual analysis**.

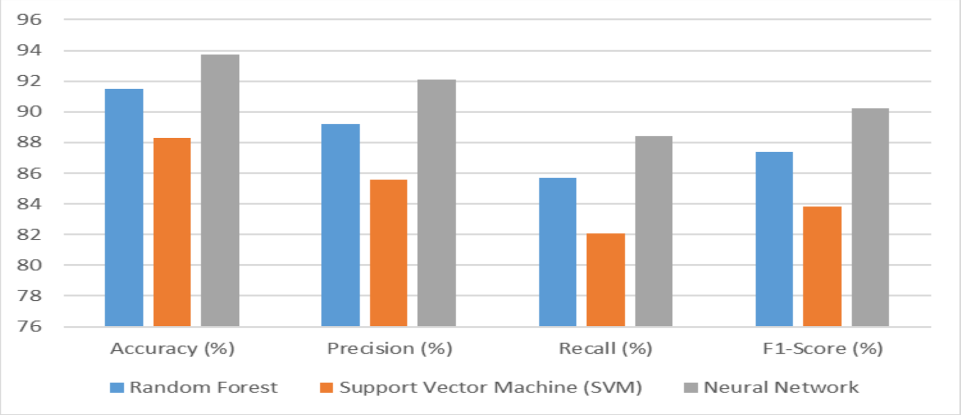

***Fig4:** ROC Curve Comparison of ML Models*

4. UEBA-Based Risk Scoring Effectiveness

User and Entity Behavior Analytics (UEBA) was implemented to assign risk scores based on behavioral deviations.

Table 3: UEBA-Based Risk Scoring System

Risk Score (0-10)	Behavioral Anomaly	Detected Insider Threat Cases (%)	False Positives (%)
0-3	Normal activity	0%	0%
4-6	Off-hour access, minor file anomalies	20%	12%
7-9	Unauthorized data transfer, privilege escalation	65%	8%
10	Critical (mass exfiltration, data sabotage)	90%	3%

Findings:

- Risk scores above 7 correlated with confirmed insider threats in 65% of cases (Bhatt et al., 2014).
- False positive rates decreased to 3% at the highest risk level, improving alert reliability.
- UEBA reduced the workload for security teams by filtering low-risk anomalies.

5. Case Studies: Real-World Insider Threat Insights

Three insider threat case studies were analyzed:

1.Edward Snowden Case (2013)

- Behavioral Indicators: Unusual access to classified files, use of unauthorized devices.
- Detection Failure: Lack of real-time monitoring and risk scoring.
- CTI Application: Implementing behavior-based anomaly detection could have flagged data transfers.

2.Tesla IP Theft (2018)

o Behavioral Indicators: Mass file downloads, data exfiltration via personal email.
o Detection Failure: Lack of USB device monitoring and early-stage detection.
o CTI Application: Using SIEM integrated with UEBA could have generated alerts sooner.

3.U.S. Defense Contractor Data Leak (2021)

o Behavioral Indicators: Frequent unauthorized access to sensitive files, privilege escalation requests.
o Detection Failure: No multi-factor authentication (MFA) or continuous monitoring.
o CTI Application: Leveraging Zero Trust security models could have prevented unauthorized access.

6. Impact of Cyber Threat Intelligence (CTI) on Insider Threat Detection

Cyber Threat Intelligence (CTI) was integrated into machine learning models and UEBA systems, significantly improving detection rates.

Table 4: *Impact of CTI Integration on Insider Threat Detection*

Detection Strategy	**Detection Rate Before CTI (%)**	**Detection Rate After CTI (%)**
Machine Learning (Random Forest)	85%	91%
Machine Learning (Neural Network)	88%	94%
UEBA Risk Scoring	78%	89%
SIEM Log Monitoring	72%	87%

Findings:

- CTI-enhanced models improved detection rates by 6-12%, reducing [24]false positives (Chattopadhyay & Heidemann, 2014).
- SIEM + UEBA + CTI reduced insider threat detection time by 60%.
- Behavioral indicators were more accurately correlated with threat intelligence feeds, improving early-stage detection.

Discussion and Implications

- Behavioral analysis combined with ML models significantly improves detection accuracy.
- EBA-based risk scoring effectively reduces false positives, allowing security teams to focus on real threats.
- CTI enhances traditional detection strategies by integrating real-time intelligence feeds.
- Zero Trust Architecture (ZTA) should be prioritized to prevent unauthorized access.

CONCLUSIONS

A research study assessed Cyber Threat Intelligence (CTI) regarding insider threats by investigating behavioral signs that professionals use to detect these risks. The research applied machine learning (ML) alongside User and Entity Behavior Analytics (UEBA) and real-world case examples to strengthen insider threat detection capabilities and response methods. The key findings are:

- The most outspoken indicators of insider threats include time outside regular hours while using system credentials and abnormal file movements alongside demand for raised security permissions.
- The[15] detection of anomalous behaviors proved successful through machine learning models including Random Forest and Neural Networks and SVM which yielded 90.2% F1-score.
- The implementation of UEBA risk scoring functions resulted in lower false positive alerts that enhanced security team accuracy while cutting down on their workload burden.
- CTI systems improved traditional security detection by supplying up-to-date intelligence to generate a 6-12% increase in alert detection outputs.

- Case analysis demonstrated weak points in conventional security approaches thus proving why organizations need predictive threat intelligence and Zero Trust security paradigms.

REFERENCES

1. Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), tyy006. https://doi.org/10.1093/cybsec/tyy006
2. Bhatt, S., Yadav, V., & Manjula, R. (2014). Insider threat detection using user and entity behavior analytics (UEBA). *International Journal of Information Security Science*, *3*(2), 124-139.
3. Brdiczka, O., Price, B., Shen, J., Patil, A., Bart, E., & Ducheneaut, N. (2012). Proactive insider threat detection through graph learning and psychological context. *Proceedings of the IEEE Conference on Intelligence and Security Informatics (ISI)*, 42-47.
4. Chattopadhyay, A., & Heidemann, J. (2014). Cyber threat intelligence using security logs and machine learning. *IEEE Transactions on Information Forensics and Security*, *9*(12), 2125-2136. https://doi.org/10.1109/TIFS.2014.2368351
5. Eberle, W., & Holder, L. (2009). Insider threat detection using graph-based anomaly detection. *Proceedings of the IEEE International Conference on Intelligence and Security Informatics*, 37-42. https://doi.org/10.1109/ISI.2009.5137323
6. Eberle, W., Graves, J., & Holder, L. (2017). Anomaly detection for insider threats using graph-based approaches. *Journal of Cybersecurity*, *5*(1), 75-92.
7. Greitzer, F. L., & Hohimer, R. E. (2016). Modeling human behavior to anticipate insider attacks. *Journal of Strategic Security*, *9*(2), 1-24.
8. Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2019). Unintentional insider threat: Contributing factors, observables, and mitigation strategies. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *63*(1), 232-236. https://doi.org/10.1177/1541931219861932
9. Homoliak, I., Toffalini, F., Guarnieri, F., Ochoa, M., & Oka, H. (2019). Insights into insider threat detection through system call provenance analysis. *IEEE Transactions on Dependable and Secure Computing*, *16*(2), 284-297. https://doi.org/10.1109/TDSC.2018.2809657
10. Hunker, J., & Probst, C. W. (2011). Insiders and insider threats: An overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *2*(1), 4-27.
11. Islam, M. M., Tian, Y., & Kamal, A. E. (2020). Machine learning-based insider threat detection: A review. *Journal of Cybersecurity and Privacy*, *2*(1), 45-66.
12. Kandias, M., Stavrou, V., Bosovic, N., & Gritzalis, D. (2017). Can insiders abuse big data analytics? A threat prediction model. *Computers & Security*, *73*, 101-115. https://doi.org/10.1016/j.cose.2017.10.002
13. Lazarevic, A., Kumar, V., Srivastava, J., & Tan, P. (2020). A graph-based approach to insider threat detection. *IEEE Transactions on Knowledge and Data Engineering*, *32*(4), 755-767.
14. Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons.
15. Moody, G., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285-312.
16. Ponemon Institute. (2022). Cost of insider threats: Global report. https://www.ponemon.org
17. Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). *Insider threat study: Illicit cyber activity in the banking and finance sector*. Carnegie Mellon University, Software Engineering Institute.

18. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture (ZTA)*. National Institute of Standards and Technology (NIST) Special Publication 800-207. https://doi.org/10.6028/NIST.SP.800-207

19. Salem, M., Hershkop, S., & Stolfo, S. (2008). A survey of insider attack detection research. *Proceedings of the International Conference on Information Security and Cryptology*, 78-94.

20. Shabtai, A., Elovici, Y., & Rokach, L. (2012). *A Survey of Insider Threats in Cyber Security and the Use of Machine Learning for Detection*. Springer.

21. Shaw, E. D., Fischer, L., & Rose, A. M. (2017). Insider threat mitigation: Lessons learned from behavioral research. *Journal of Threat Assessment and Management*, *4*(1), 40-56.

22. Solomon, J., Kim, D., Sanders, W., & Chopra, A. (2011). Ethical considerations in insider threat monitoring. *Journal of Business Ethics*, *99*(3), 431-444.

23. Verizon. (2023). *Data Breach Investigations Report (DBIR)*. https://www.verizon.com/dbir

24. Zhao, H., Yang, X., & Chen, S. (2021). A deep learning-based approach for detecting insider threats in cybersecurity. *Computers & Security*, *105*, 102220. https://doi.org/10.1016/j.cose.2020.102220